(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 septembre 2001 (27.09.2001)

PCT

(10) Numéro de publication internationale
WO 01/71675 A1

(51) Classification internationale des brevets[7] : G07F 7/12, H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR01/00808

(22) Date de dépôt international : 19 mars 2001 (19.03.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/03684 22 mars 2000 (22.03.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GILBERT, Henri** [FR/FR]; 2, allée des Peupliers, F-91440 Bures sur Yvette (FR). **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR).

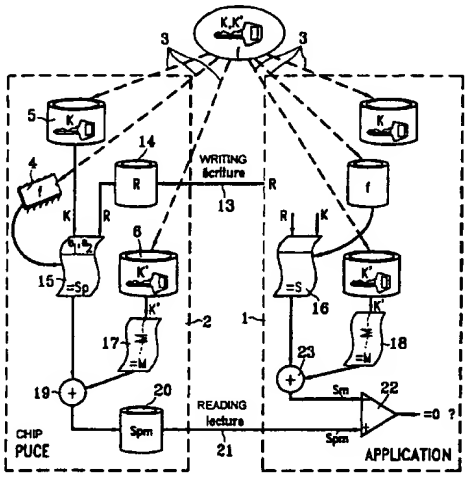
(74) Mandataire : **LEMOYNE, Didier**; France Telecom R & D/VAT/VPI, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(national)* : JP, US.

*[Suite sur la page suivante]*

(54) Title: CRYPTOGRAPHIC METHOD FOR PROTECTION AGAINST FRAUD

(54) Titre : PROCEDE CRYPTOGRAPHIQUE DE PROTECTION CONTRE LA FRAUDE




(57) **Abstract:** The invention concerns a cryptographic method for protection against fraud in transactions between an application (1) and a user's electronic chip (2). The method consists in: calculating (15, 16) a certificate (Sp, S), with the electronic chip (2) and the application (1), the certificate (Sp, S) being the result of the non-linear function f applied to a list of arguments ($e_1$, $e_2$) comprising at least the variate R and the secret key K; attributing to the electronic chip (2) a second secret key K' known only to the electronic chip (2) and the application (1), and kept secret (6) in the electronic chip (2); each time the electronic chip (2) is authenticated, determining (17, 18) a mask M calculated at least partly from the secret key K'; masking (19) the value of the certificate (Sp) using the mask M to make available to the application (1) only the value of the masked certificate (Spm); verifying with the application (1) the masked value (Spm) of the certificate calculated by the electronic chip (2).

(57) **Abrégé :** La présente invention se rapporte à un procédé cryptographique de protection contre la fraude dans des transactions entre une application (1) et une puce électronique (2) d'un utilisateur. Le procédé consiste: à calculer (15, 16) un certificat (Sp, S), par la puce électronique (2) et l'application (1), le certificat (Sp, S) étant le résultat de la fonction non linéaire f appliquée à une liste d'arguments ($e_1$, $e_2$)

*[Suite sur la page suivante]*

WO 01/71675 A1

(84) **États désignés** *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

**Publiée :**

— *avec rapport de recherche internationale*

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

comprenant au moins l'aléa R et la clé secrète K, à attribuer à la puce électronique (2) une seconde clé secrète K' connue seulement de la puce électronique (2) et de l'application (1), et gardée secrète (6) dans la puce électronique (2), à chaque authentification de la puce électronique (2) à déterminer (17, 18) un masque M calculé à partir d'au moins une partie de la clé secrète K', à masquer (19) la valeur du certificat (Sp) au moyen du masque M pour rendre disponible à l'application (1) uniquement la valeur du certificat masquée (Spm), à vérifier par l'application (1) la valeur masquée (Spm) du certificat calculée par la puce électronique (2).

Titre de l'invention

# PROCEDE CRYPTOGRAPHIQUE DE PROTECTION CONTRE LA FRAUDE

Domaine de l'invention

La présente invention se rapporte à un procédé cryptographique de protection contre la fraude d'une puce électronique.

L'invention trouve une application très avantageuse en ce qu'elle permet de protéger contre la fraude des puces à circuit intégré à logique câblée ou à microprocesseur, notamment les puces qui équipent les cartes prépayées utilisées dans des transactions diverses telles que l'établissement de communications téléphoniques, le paiement d'objets dans un distributeur automatique, la location d'emplacements de stationnement à partir d'un parcmètre, le paiement d'un service comme un transport public ou comme la mise à disposition d'infrastructures (péage, musée, bibliothèque,...).

Description de l'art antérieur

Actuellement, les cartes prépayées sont susceptibles de subir différents types de fraude. Un premier type de fraude consiste à dupliquer sans autorisation la carte, le terme clonage étant souvent utilisé pour caractériser cette opération. Un deuxième type de fraude consiste à modifier les données attachées à une carte, en particulier le montant du crédit inscrit dans la carte. Pour lutter contre ces fraudes il est fait appel à la cryptographie, d'une part pour assurer l'authentification de la carte au moyen d'une authentification et/ou pour assurer l'authentification des données au moyen d'une signature numérique et, d'autre part pour assurer le cas échéant la confidentialité des données au moyen d'un chiffrement. La cryptographie met en jeu deux entités, un vérificateur et un objet à vérifier, et elle peut être soit symétrique, soit asymétrique. Lorsqu'elle est symétrique, les deux entités partagent exactement la même information, en particulier une clé secrète. Lorsqu'elle est asymétrique une des deux entités possède une paire de clés dont l'une est secrète et l'autre est publique ; il n'y a pas de clé secrète partagée. Dans de nombreux systèmes, seule la cryptographie symétrique est mise en œuvre avec des cartes prépayées, car la cryptographie asymétrique reste lente et coûteuse. Les premiers mécanismes d'authentification développés en cryptographie symétrique consistent à calculer une fois pour toutes un certificat, différent pour chaque carte, à le stocker dans la mémoire de la carte, à le lire à chaque transaction et à le vérifier en interrogeant une application du réseau supportant la transaction où sont stockés les certificats déjà attribués. Ces mécanismes assurent une protection

insuffisante, d'une part parce que le certificat peut être espionné, reproduit et rejoué frauduleusement étant donné qu'il est toujours le même pour une carte donnée et, d'autre part parce que les cartes peuvent être clonées. Pour lutter contre les clones, les mécanismes d'authentification passifs de cartes sont remplacés par des mécanismes d'authentification actifs qui peuvent en outre assurer l'intégrité des données. Un premier de ces mécanismes fait l'objet du brevet FR 89 09734. Le procédé décrit consiste à déterminer une fonction non linéaire, cette fonction étant connue de l'application et implantée dans une puce électronique sous la forme d'un automate d'états. Lors d'une authentification, la puce électronique et l'application calculent un certificat qui est le résultat de la fonction appliquée à une liste d'arguments déterminée à chaque authentification ; la liste d'arguments pouvant comprendre un aléa, l'aléa étant une donnée déterminée par l'application à chaque authentification, une donnée contenue dans la puce électronique et une clé secrète connue de la puce électronique et de l'application. Lorsque le certificat calculé par la puce électronique est identique au certificat calculé par l'application, la puce électronique est jugée authentique et la transaction entre la puce électronique et l'application est autorisée. Un second mécanisme de protection des cartes par authentification active inconditionnellement sûre, basé sur l'utilisation pour un nombre limité d'authentifications d'une fonction linéaire assurant une protection contre le rejeu et une usure contrôlée de la clé secrète, fait l'objet du brevet FR 95 12144.

Toutefois, chacun des deux mécanismes précédemment cités possède des avantages et des inconvénients spécifiques. En ce qui concerne le premier mécanisme, qui repose sur l'hypothèse (non prouvable dans l'état actuel des connaissances) de la sécurité informatique de la fonction non linéaire utilisée, les très fortes contraintes imposées par les capacités de calculs réduites des puces à logique câblée n'autorisent pas une marge de sécurité aussi large que pour les algorithmes à clé secrète usuels et, de ce fait la divulgation de la spécification détaillée de la fonction non linéaire utilisée peut représenter un risque. En ce qui concerne le second mécanisme, il possède l'avantage de bénéficier d'une sécurité prouvable tant que le nombre d'authentifications n'excède pas un certain seuil, et il n'y a donc pas de risque lié à la divulgation de la fonction linéaire utilisée mais, par contre la nécessité de limiter strictement le nombre d'utilisations de la fonction d'authentification pour la durée de vie de la puce (ou dans le cas de cartes rechargeables, entre deux rechargements) inhérente à cette solution peut représenter une contrainte difficile à satisfaire pour certaines applications. En outre, des attaques portant non pas sur les puces à logique câblée mais, sur les modules de sécurité

utilisés pour la vérification de ces puces et, selon lesquelles un fraudeur fournirait à des modules de vérification des réponses aléatoires jusqu'à ce qu'un nombre suffisant de bonnes réponses, obtenues par hasard, lui fournisse le secret associé à un numéro de carte de son choix, peuvent être plus difficiles à contrer dans le cas du second mécanisme.

Résumé de l'invention

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé cryptographique de protection contre la fraude d'une puce électronique qui comprend les étapes consistant :

- à déterminer une fonction non linéaire connue de l'application et implantée dans la puce électronique,
- à attribuer à la puce électronique une première clé secrète K, connue seulement de la puce électronique et de l'application, et gardée secrète dans la puce électronique,
- à chaque authentification de la puce électronique à générer par l'application un mot d'entrée R appelé aléa,
- à calculer un certificat S, par la puce électronique et l'application, le certificat étant le résultat de la fonction non linéaire appliquée à une liste d'arguments comprenant au moins l'aléa R et la clé secrète K,

et qui assure une sécurité accrue en conservant les avantages des mécanismes mentionnés précédemment tout en évitant tout ou partie de leurs inconvénients.

Une solution au problème technique posé consiste, selon la présente invention, en ce que ledit procédé comprend en outre les étapes consistant :

- à attribuer à la puce électronique une seconde clé secrète K' connue seulement de la puce électronique et de l'application, et gardée secrète dans la puce électronique,
- à chaque authentification de la puce électronique à déterminer un masque M calculé à partir d'au moins une partie de la clé secrète K',
- à masquer la valeur du certificat S au moyen du masque M pour rendre disponible à l'application uniquement la valeur du certificat masquée,
- à vérifier par l'application la valeur masquée du certificat calculée par la puce électronique.

Ainsi, le procédé selon l'invention, qui concerne la protection contre la fraude dans des transactions entre une puce électronique et une application, masque la valeur du certificat S calculée par la puce électronique, avant que l'application le lise pour en

vérifier sa valeur et déterminer si la puce électronique est authentique ; le calcul du certificat S et la détermination du masque M faisant intervenir respectivement, une première clé et une seconde clé gardées secrètes dans la puce électronique et connues de l'application.

Le procédé conforme à l'invention résout le problème posé, d'une part car la valeur de certificat S est protégée par masquage et, par conséquent la sécurité de la méthode d'authentification active selon l'invention repose sur des hypothèses de sécurité beaucoup moins fortes que lorsque la valeur de certificat S n'est pas protégée par masquage et, d'autre part car l'utilisation d' une fonction non linéaire informatiquement sûre permet de prolonger la protection des secrets utilisés au-delà du seuil où la sécurité inconditionnelle de ces secrets est compromise.

L'application vérifie l'exactitude de la valeur masquée, soit en démasquant le certificat masqué calculé par la puce électronique au moyen de la fonction inverse du masque et en comparant la valeur démasquée à la valeur du certificat calculé par l'application, soit, après avoir calculé les valeurs du certificat S et du masque M, en masquant au moyen du masque M la valeur du certificat S et en comparant cette valeur masquée à celle calculée par la puce électronique. Lorsque les valeurs comparées sont identiques, la puce électronique est jugée authentique et la transaction entre la puce et l'application est autorisée.

De manière avantageuse, un mode particulier de mise en œuvre permet d'assurer simultanément l'authentification de la carte et l'authentification de données en faisant intervenir la valeur de certaines données dans le calcul du certificat. Dans un premier cas, ces données peuvent être mémorisées dans la puce électronique et être constituées par le numéro de la puce ou par un crédit associé à la puce électronique. Dans un second cas, ces données sont écrites dans la puce par l'application lors de l'opération d'authentification.

Selon un mode particulier de mise en œuvre, la détermination d'une clé peut être effectuée par l'application par une méthode de diversification avec pour arguments d'entrée le numéro de la puce électronique et un code secret maître, ce qui permet avantageusement à l'application de reconstituer les clés secrètes de chaque puce électronique après lecture du numéro de la puce ; aucun stockage des clés secrètes des puces n'est nécessaire.

L'attribution des clés à une puce électronique est effectuée, soit lors de la personnalisation de la puce en fin de fabrication, soit lors d'une opération de rechargement de la puce dans le cas d'une puce rechargeable. Bien qu'il soit préférable

d'utiliser des clés K et K' indépendantes, il peut exister un lien de dépendance entre la première clé K et la seconde clé K' d'une puce électronique ; ce lien pouvant se présenter sous la forme d'une fonction qui permet de calculer la clé K' à partir de la clé K, ou la clé K' à partir de la clé K.

Dans un mode particulier de mise en œuvre, la clé K' est un mot d'un nombre déterminé de bits regroupés en séquence ; chaque séquence ayant un nombre de bits égal au nombre de bits qui compose le masque M. Le masque M est déterminé par le choix, différent à chaque authentification, d'une de ces séquences. Le choix peut être effectué en pointant sur les séquences au moyen d'un pointeur positionné par la valeur d'un compteur implanté dans la puce ou positionné par la valeur d'un paramètre fourni par l'application lors de l'authentification. Dans un autre mode de mise en œuvre, chaque bit constituant le masque M est égal à une combinaison linéaire modulo 2 de bits de la clé K' ; la combinaison étant calculée à chaque authentification, d'une part par l'application et d'autre part par la puce.

Brève description des dessins

D'autres caractéristiques et avantages de l'invention apparaîtront lors de la description qui suit de modes particuliers de réalisation ; la description étant faite en regard de dessins annexés donnés à titre d'exemples non limitatifs.

La figure 1 est un schéma d'un procédé selon l'invention.

La figure 2 est un schéma d'une fonction non linéaire f.

Description d'un mode de réalisation

La figure 1 représente schématiquement un procédé cryptographique selon l'invention, de protection contre la fraude dans des transactions entre une application 1 et une puce électronique 2 d'un utilisateur.

L'application 1 peut être entièrement ou partiellement délocalisée dans un terminal en libre service non surveillé, tel un téléphone public ou tel un tourniquet d'accès à un transport public. L'utilisateur détient une puce électronique 2, implantée par exemple sur une carte prépayée, qui doit lui permettre d'établir une transaction avec l'application 1. Ces transactions peuvent consister en l'établissement de communications téléphoniques, le paiement d'objets dans un distributeur automatique, la location d'emplacements de stationnement à partir d'un parcmètre, le paiement d'un service comme un transport public ou comme la mise à disposition d'infrastructures.

Le procédé permet soit d'authentifier la puce électronique 2, soit d'authentifier l'application 1 ; le fraudeur falsifiant soit la puce électronique 2 au moyen d'un clone, soit l'application 1 au moyen d'un faux terminal.

La puce électronique 2 est personnalisée au moment de sa fabrication et, éventuellement lors d'une opération de rechargement, au moyen d'un numéro d'identité i et d'une valeur initiale d'une donnée D liée à l'application 1 à laquelle elle est destinée ; la valeur D représente généralement le crédit attaché à la puce électronique 2 pour une application 1 donnée.

Le procédé consiste, lors de cette opération de personnalisation ou, lors d'une opération préalable à la commercialisation de la puce électronique, à déterminer 3 les conditions initiales nécessaires à l'authentification, soit de la puce électronique 2, soit de l'application 1. Ces conditions initiales comprennent la détermination d'une fonction non linéaire f, d'une première clé secrète K et d'une seconde clé secrète K'. La fonction non linéaire f est connue de l'application 1 et elle est implantée dans la puce électronique 2 sous la forme de circuits électroniques 4 ou, dans le cas de puces électroniques dotées d'un microprocesseur, sous la forme d'un programme. La première clé K, respectivement la seconde clé K', est conservée secrètement dans une mémoire 5, respectivement 6, de la puce électronique 2.

La fonction non linéaire f peut être implantée sous la forme d'une succession de registres formant un registre à décalage, associés à une mémoire et à des opérateurs ou exclusifs ; une telle fonction est dite « automate d'états » et un exemple est représenté à la figure 2. Suivant cet exemple, la fonction f consiste en un premier opérateur ou exclusif 7, un registre à décalage 4 bits comprenant quatre bascules r0 à r3 et quatre opérateurs ou exclusifs 8 à 11 et, en une mémoire 12 de taille 16x4 bits. Chaque opérateur ou exclusif 7 à 11 a deux entrées et une sortie. Chaque bascule r0 à r3 a une entrée de données, deux sorties de données et une entrée horloge non représentée. La mémoire 12 a quatre entrées et quatre sorties et une entrée horloge non représentée. Les arguments d'entrée $e_1, e_2$ qui comprennent au moins la première clé secrète K et une seconde valeur R sont présents sur une des entrées du premier opérateur ou exclusif 7. La sortie du premier opérateur ou exclusif 7 est connectée à la première entrée du deuxième opérateur ou exclusif 8. L'entrée des bascules r0, r1, r2 et r3 est connectée à la sortie d'un opérateur ou exclusif 8 à 11. La première sortie des bascules r0, r1 et r2 est connectée à une première entrée d'un opérateur ou exclusif 9 à 11. La seconde sortie des bascules r0, r1, r2 et r3 est connectée à une entrée de la mémoire 12. La seconde entrée des opérateurs ou exclusifs 8 à 11 est connectée à une sortie de la mémoire 12. La première sortie de la bascule r3 donne la valeur du certificat S calculée par la fonction f appliquée aux arguments $e_1, e_2$ qui comprennent au moins la première clé secrète K et une seconde valeur R. A chaque authentification de la puce

électronique 2 ou, de l'application 1, correspond un nombre de coups d'horloge égal au nombre de bits des arguments d'entrée $e_1, e_2$ ; les bits du résultat S sortent en série à chaque coup d'horloge.

La première clé K, généralement attribuée de manière individuelle à une puce électronique 2, consiste typiquement en un mot de 64 à 128 bits ; ce mot est connu de l'application 1 et est gardé 5 secret dans la puce électronique 2. Cependant, selon un mode particulier de réalisation du procédé, l'application 1 ne mémorise pas la clé K elle-même mais un secret dit maître. Ce secret maître est tel qu'il permet de reconstituer, par une méthode dite de diversification, la clé K à partir du numéro i d'identité de la puce électronique 2.

Quel que soit le mode de réalisation du procédé, la clé K est typiquement conservée dans la puce électronique 2 dans une mémoire morte telle une PROM 5. En particulier, lorsque la puce électronique 2 est de type rechargeable, c'est le cas d'une puce électronique 2 implantée sur une carte prépayée à rechargement, la mémoire morte 5 est aussi accessible en écriture, telle une EEPROM.

La seconde clé K' se présente comme la clé K, sous la forme d'un mot d'un certain nombre de bits. Les clés K et K' sont mémorisées dans la puce électronique 2, dans la même mémoire à des adresses différentes ou dans deux mémoires distinctes 5, 6, et, la détermination des bits de K', respectivement de K, peut dans certains cas dépendre de la clé K, respectivement K'.

Après l'opération de personnalisation, la puce électronique 2 est commercialisée et l'utilisateur peut entreprendre une transaction avec une application 1. Deux cas peuvent se présenter suivant que l'authentification consiste à authentifier la puce électronique 2 par l'application 1 ou, suivant que l'authentification consiste à authentifier l'application 1 par la puce électronique 2.

Le premier cas correspond au schéma de la figure 1. Dans ce cas, l'application 1 cherche à déterminer si la puce électronique 2 est authentique ou pas ; en effet, il peut s'agir du clone d'une puce électronique 2.

Dans une première étape du procédé, l'application 1 génère un mot R appelé aléa. Le mot R comprend un nombre de bits déterminé pour éviter toute tentative frauduleuse de rejeu ; typiquement le nombre de bits est de l'ordre de quelques dizaines de bits. Le mot R est généré à l'aide d'un générateur aléatoire ou d'un générateur pseudo-aléatoire. Dans un mode particulier de réalisation, les mots R successivement générés peuvent consister en une suite d'entiers consécutifs prédictibles. Le mot R est un argument d'entrée pour le calcul du certificat Sp, S effectué par la puce électronique

2 et par l'application 1. Pour que la puce électronique 2 ait accès au mot R, l'application 1 effectue une écriture 13 dans la puce électronique 2 ou la puce électronique 2 vient lire le mot R dans l'application 1. L'échange entre la puce électronique 2 et l'application 1 peut s'effectuer suivant un protocole établi lors de la personnalisation de la puce électronique 2 ; la valeur R peut, par exemple, être codée. Le mot R est stocké temporairement dans une mémoire 14 tampon de la puce électronique 2, ainsi que dans l'application 1.

Dans une deuxième étape du procédé, l'application 1 d'une part et, la puce électronique 2 d'autre part, calculent 15, 16 un certificat noté respectivement S et Sp. Le certificat S, respectivement Sp, est le résultat du calcul effectué par la fonction non linéaire f appliquée à une liste d'arguments $e_1, e_2$ qui comprend au moins l'aléa R et la clé K. Dans des modes particuliers de réalisation du procédé, la liste d'arguments $e_1, e_2$ comprend en outre, le numéro i d'identité de la puce ou, la valeur de la donnée D contenue dans la puce ou, la valeur d'une donnée D' générée par l'application et écrite dans la puce avant l'authentification ou, une combinaison des arguments précédents.

Dans une troisième étape, le procédé consiste à déterminer 17, 18 un masque M à partir d'au moins une partie de la clé K'. Le masque M consiste en un nombre déterminé m de bits qui est typiquement égal à une dizaine de bits. Le nombre de bits de M est de préférence le même que le nombre de bits du certificat S, pour masquer totalement le certificat S et ne révéler aucune information sur le certificat S. La détermination de M peut être effectuée de différentes manières. Dans un premier mode de réalisation, la détermination de M consiste à sélectionner m bits successifs de la clé K' et à décaler de m, après chaque authentification, le rang du premier bit sélectionné. Ainsi, lors de la première authentification, le masque M comprend les bits $b_0, b_1, ..., b_{m-1}$ et lors de l'authentification suivante le masque M comprend les bits $b_m, b_{m+1}, ..., b_{2m-1}$ avec $b_0, b_1, ..., b_{n-1}$ les bits de la clé K'. Dans un deuxième mode de réalisation, la détermination de M consiste à effectuer une combinaison des bits de la clé K' ; par exemple, si $m_0, m_1, ..., m_{m-1}$ sont les bits de M, si $b_0, b_1, ..., b_{n-1}$ sont les bits de la clé K'et si l'aléa R peut être décomposé en m mots de n bits $R_0 = r_{0,0}, r_{0,1}, .., r_{0,n-1}$ ; $R_1 = r_{1,0}, r_{1,1}, .., r_{1,n-1}$ ; $R_{m-1} = r_{m-1,0}, r_{m-1,1}, .., r_{m-1,n-1}$, alors : $m_i = (b_0.r_{i,0} + b_1.r_{i,1} + ... + b_{n-1}.r_{i,n-1}) \bmod 2$ Dans un troisième mode de réalisation qui généralise le premier mode de réalisation mentionné ci-dessus, la détermination de M consiste à déterminer un paramètre c et à sélectionner une séquence de bits de la clé K' en pointant les bits de K' au moyen de c. Ceci nécessite de considérer la clé K' comme

une suite de séquences de bits. Ainsi, si $m_0, m_2, ..., m_{m-1}$ sont les bits de M et si K' est une suite de séquences de m bits, K' peut se représenter sous la forme d'un tableau :

| | | | |
|---|---|---|---|
| $b_0$ | $b_m$ | ... | $b_{n-m}$ |
| ... | ... | ... | ... |
| $b_{m-1}$ | $b_{2m-1}$ | ... | $b_{n-1}$ |

et le contenu d'une colonne peut être représentée par le mot de m bits K'[i], avec i=1 à n/m. Dans ces conditions, M est égal à K'[c] où c est un paramètre appartenant à l'intervalle [1, n/m]. Selon un premier mode de réalisation, la valeur du paramètre c est déterminée par la valeur d'un compteur, implanté dans la puce et incrémenté à chaque authentification de la puce, et, l'application accède à la valeur du compteur en effectuant une lecture dans la puce. Selon un second mode de réalisation, la valeur du paramètre c dépend simultanément de la valeur d'un compteur, implanté dans la puce et incrémenté à chaque authentification de la puce, et, par exemple, de l'aléa R. La valeur de c peut aussi dépendre de la valeur D ou de la valeur D' ou du numéro i d'identité de la puce.

Dans une quatrième étape du procédé, la puce électronique 2 masque 19 la valeur du certificat Sp qu'elle a calculée 17 au moyen du masque M. Dans un premier mode de réalisation, le masquage 19 est calculé au moyen d'une fonction de chiffrement. Une fonction de chiffrement est une fonction bijective paramétrée par une clé qui, à un ensemble de valeurs, fait correspondre un autre ensemble de valeurs ; par exemple la fonction F : $x \rightarrow x + k$ modulo 2, avec x=0 ou 1 et k = 0 ou 1 peut être utilisée comme fonction de chiffrement. La fonction de chiffrement peut consister en une opération ou exclusif entre le certificat Sp et le masque M. Le résultat de l'opération de masquage donne la valeur du certificat masquée Spm qui est stockée de manière temporaire dans une mémoire 20 tampon de la puce électronique 2.

Dans une cinquième étape du procédé, l'application 1 effectue une lecture 21 de la mémoire 20 tampon, ou la puce électronique 2 vient écrire le certificat masqué Spm dans l'application 1. L'échange 21 entre la puce électronique 2 et l'application 1 peut s'effectuer suivant un protocole similaire à celui utilisé pour l'échange de l'aléa R. L'application 1 vérifie ensuite la valeur Spm du certificat masqué calculée par la puce électronique 2 en la comparant 22 à la valeur S du certificat qu'elle a elle-même calculée 16. Pour effectuer la comparaison 22, soit l'application 1 masque 23 la valeur S au moyen du masque M qu'elle 1 a préalablement calculé 18 pour obtenir une valeur masquée Sm et la comparer 22 à la valeur Spm comme représenté sur la figure 1, soit

l'application démasque la valeur Spm en faisant intervenir une fonction inverse du masque pour obtenir la valeur Sp et la comparer à la valeur S.

Un mode particulier de réalisation du procédé limite le nombre d'authentifications pouvant être effectuées pour une même puce électronique. Cette limitation permet avantageusement de protéger les puces électroniques contre des attaques d'un fraudeur qui consistent à tirer parti de l'observation d'un nombre d'authentifications supérieur à ce qui est requis par l'application. Selon ce mode de réalisation, la puce comprend en mémoire un nombre V déterminé en fonction de l'application et égal au nombre maximum d'authentifications de la puce. Lorsqu'une opération d'authentification se présente, la transaction demandée est interdite si la puce a préalablement effectué un nombre V d'authentifications. Pour contrôler le nombre d'authentifications déjà effectuées, la puce contient typiquement un compteur incrémenté à chaque opération d'authentification. Lorsque le compteur atteint la valeur V, il déclenche un verrouillage interne de la puce pour lui interdire d'effectuer tout nouveau calcul de certificat. En l'absence de valeur de certificat calculée par la puce, la vérification de certificat effectuée par l'application échoue et par conséquent l'application interdit la transaction avec la puce.

Une variante du procédé précédemment décrit en regard des figures 1 et 2 permet avantageusement de remédier à certaines tentatives de piratage consistant à simuler vis à vis d'une puce le comportement d'une application, à l'aide d'une authentification de l'application par la puce. Selon cette variante, des opérations précédemment effectuées par l'application sont effectuées par la puce électronique et vice versa. Ainsi :

- à chaque authentification de l'application, le mot d'entrée R appelé aléa est généré par la puce électronique et non par l'application,
- le masque M est déterminé de part et d'autre à chaque authentification de l'application,
- l'application calcule un certificat et le masque au moyen du masque M pour rendre disponible à la puce électronique uniquement la valeur du certificat masquée,
- l'opération de comparaison des valeurs de certificat calculées d'une part par la puce et, d'autre part par l'application est effectuée par la puce électronique.

## REVENDICATIONS

1. Procédé cryptographique de protection contre la fraude dans des transactions entre une application (1) et une puce électronique (2) d'un utilisateur comprenant les étapes consistant :

   - à déterminer une fonction non linéaire f connue de l'application (1) et implantée (4) dans la puce électronique (2),
   - à attribuer à la puce électronique (2) une première clé secrète K, connue seulement de la puce électronique (2) et de l'application (1), et gardée secrète (5) dans la puce électronique (2),
   - à chaque authentification de la puce électronique (2) à générer un mot R d'entrée variable appelé aléa,
   - à calculer (15, 16) un certificat (Sp, S), par la puce électronique (2) et l'application (1), le certificat (Sp, S) étant le résultat de la fonction non linéaire f appliquée à une liste d'arguments $(e_1, e_2)$ comprenant au moins l'aléa R et la clé secrète K, caractérisé en ce que ledit procédé comprend en outre les étapes consistant :
   - à attribuer à la puce électronique (2) une seconde clé secrète K' connue seulement de la puce électronique (2) et de l'application (1), et gardée secrète (6) dans la puce électronique (2),
   - à chaque authentification de la puce électronique (2) à déterminer (17, 18) un masque M calculé à partir d'au moins une partie de la clé secrète K',
   - à masquer (19) la valeur du certificat (Sp) au moyen du masque M pour rendre disponible à l'application (1) uniquement la valeur du certificat masquée (Spm),
   - à vérifier par l'application (1) la valeur masquée (Spm) du certificat calculée par la puce électronique (2).

2. Procédé selon la revendication 1, caractérisé en ce que la vérification par l'application (1) de la valeur masquée (Spm) du certificat calculée par la puce électronique (2) consiste :

   - à démasquer au moyen du masque M la valeur masquée (Spm) du certificat calculée par la puce électronique (2) et,
   - à comparer la valeur du certificat (Sp) calculée par la puce électronique (2) à celle (S) calculée par l'application (1).

3. Procédé selon la revendication 1, caractérisé en ce que la vérification par l'application (1) de la valeur masquée (Spm) du certificat calculée par la puce électronique (2) consiste :

   - à masquer (23) au moyen du masque M la valeur du certificat (S) calculée par l'application (1) et,
   - à comparer (22) la valeur masquée du certificat (Spm) calculée par la puce électronique (2) à la valeur masquée du certificat (Sm) calculée par l'application (1).

4. Procédé selon la revendication 1, caractérisé en ce que l'aléa R est déterminé par l'application (1) à partir d'un nombre aléatoire généré par l'application (1) et en ce que l'aléa R est transmis à la puce électronique (2) par l'application (1).

5. Procédé selon la revendication 1, caractérisé en ce que l'aléa R est déterminé à partir d'une suite d'entiers consécutifs générés par l'application (1) et par la puce électronique (2).

6. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) est le résultat de la fonction non linéaire f appliquée à une liste d'arguments $(e_1, e_2)$ comprenant au moins l'aléa R, la clé secrète K et des données D internes à la puce électronique.

7. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) est le résultat de la fonction non linéaire appliquée à une liste d'arguments $(e_1, e_2)$ comprenant au moins l'aléa R, la clé secrète K et des données D' fournies à la puce électronique (2) par l'application (1) lors de l'authentification.

8. Procédé selon la revendication 1, caractérisé en ce que les clés secrètes K et K' sont choisies indépendamment l'une de l'autre.

9. Procédé selon la revendication 1, caractérisé en ce que K' consiste en une séquence de valeurs K'[i] et que M est égal à une combinaison linéaire modulo 2 des bits des valeurs K'[i], combinaison dont les caractéristiques sont déterminées au moment de la procédure d'authentification.

10. Procédé selon la revendication 1, caractérisé en ce que K' consiste en une séquence de valeurs K'[i] et que M est égal à la valeur K'[c] prise parmi les valeurs K'[i] et déterminée par le choix d'un paramètre c effectué au moment de l'authentification.

11. Procédé selon la revendication 10, caractérisé en ce que la valeur du paramètre c est calculée à partir d'au moins la valeur d'un compteur contenu dans la puce électronique et incrémenté à chaque authentification.

12. Procédé selon la revendication 10, caractérisé en ce que la valeur du paramètre c est calculée à partir d'au moins la valeur d'un compteur contenu dans la puce électronique et incrémenté à chaque authentification et de l'aléa R.

13. Procédé selon la revendication 1, caractérisé en ce que le masquage du certificat S au moyen du masque M est calculé au moyen d'une fonction de chiffrement (F).

14. Procédé selon la revendications 13, caractérisé en ce que la fonction de chiffrement (F) est une opération OU Exclusif bit à bit.

15. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) et le masque M ont le même nombre de bits.

16. Procédé selon la revendication 1, caractérisé en ce que le nombre d'authentifications de la puce électronique (2) est limité à une valeur maximale V déterminée par l'application (1) et inscrite dans la puce électronique (2).

17. Procédé selon la revendication 16, caractérisé en ce que la puce électronique (2) contient un compteur incrémenté à chaque authentification, et que la puce électronique (2) cesse tout calcul d'authentification lorsque la valeur du compteur atteint la valeur maximale V.

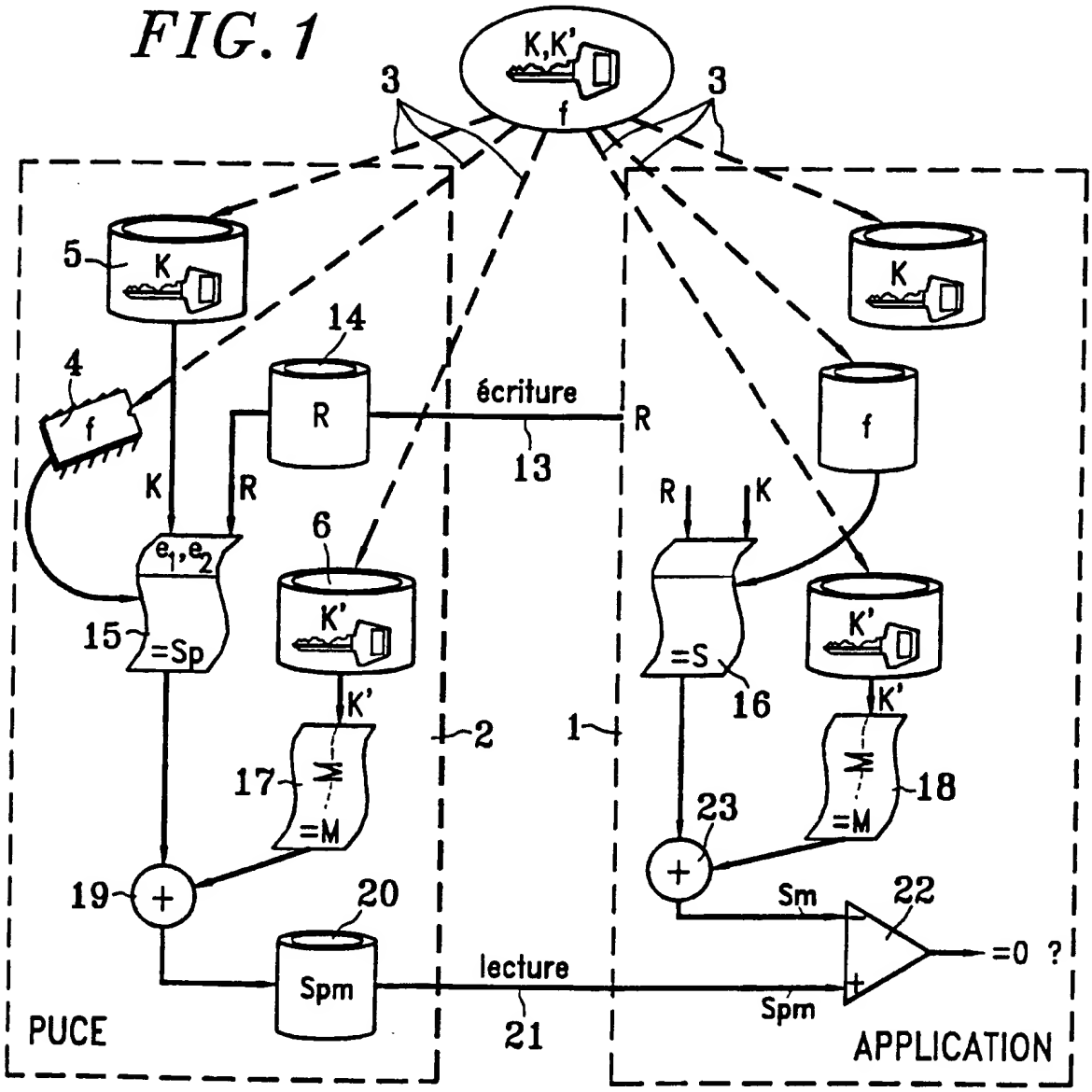
18. Procédé cryptographique de protection contre la fraude dans des transactions entre une application (1) et une puce électronique (2) d'un utilisateur comprenant les étapes consistant :

- à déterminer une fonction non linéaire f connue de l'application (1) et implantée (4) dans la puce électronique (2),
- à attribuer à la puce électronique (2) une première clé secrète K, connue seulement de la puce électronique (2) et de l'application (1), et gardée secrète (5) dans la puce électronique,
- à chaque authentification de l'application (1) à générer un mot d'entrée R appelé aléa,
- à calculer un certificat (Sp, S), par la puce électronique (2) et l'application (1), le certificat (Sp, S) étant le résultat de la fonction non linéaire f appliquée à une liste d'arguments $(e_1, e_2)$ comprenant au moins l'aléa R et la clé secrète K, caractérisé en ce que ledit procédé comprend en outre les étapes consistant :
- à attribuer à la puce électronique (2) une seconde clé secrète K', connue seulement de la puce électronique (2) et de l'application (1), et gardée secrète (6) dans la puce électronique (2),
- à chaque authentification de l'application (1) à déterminer un masque M calculé à partir d'au moins une partie de la clé secrète K',
- à masquer la valeur du certificat (S) au moyen du masque M pour rendre disponible à la puce électronique (2) uniquement la valeur du certificat (S) masquée (Sm),
- à vérifier par la puce électronique (2) la valeur masquée (Sm) du certificat (S) calculée par l'application (1).

19. Procédé selon la revendication 18, caractérisé en ce que l'aléa R est déterminé par la puce électronique (2) à partir d'un nombre aléatoire généré par la puce électronique (2) et en ce que l'aléa R est transmis à l'application (1) par la puce électronique (2).

20. Procédé selon la revendication 18, caractérisé en ce que l'aléa R est déterminé à partir d'une suite d'entiers consécutifs générés par l'application (1) et par la puce électronique (2).

FIG. 1


K,K'
f
3
3
5
K
14
R
écriture
R
13
4
f
K
R
6
e1,e2
15
=Sp
K'
17
=M
2
1
R
K
=S
16
K'
18
=M
23
19
20
Spm
lecture
21
Sm
22
=0 ?
Spm
PUCE
APPLICATION

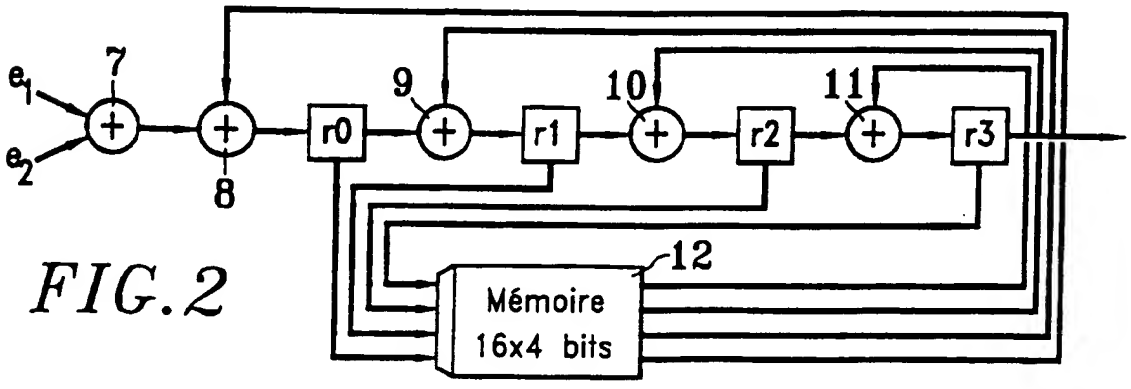

e1
e2
7
8
9
10
11
r0
r1
r2
r3
12
Mémoire
16x4 bits

FIG. 2

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/F.. 01/00808

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/12 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 97 22093 A (LANDIS & GYR)<br>19 June 1997 (1997-06-19)<br>abstract; claims; figure 1<br>page 2, line 25 -page 3, line 28 | 1,3,4,6,<br>13-15 |
| A | EP 0 565 279 A (AMERICAN TELEPHONE AND TELEGRAPH) 13 October 1993 (1993-10-13)<br>abstract; claims; figure 5<br>page 5, line 9 - line 33 | 1,2,4,6 |
| A | EP 0 621 570 A (FRANCE TELECOM)<br>26 October 1994 (1994-10-26)<br>the whole document | 1,4,6,7,<br>10-12 |
| A | DE 41 38 861 A (SIEMENS NIXDORF INFORMATIONSSYSTEME)<br>1 October 1992 (1992-10-01)<br>the whole document | 1,4,6,<br>18,19 |

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 25 June 2001 | 04/07/2001 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

1

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/F[illegible] 01/00808

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9722093 A | 19-06-1997 | CH 690530 A | 29-09-2000 |
| | | AU 704773 B | 06-05-1999 |
| | | AU 1140497 A | 03-07-1997 |
| | | EP 0870286 A | 14-10-1998 |
| EP 0565279 A | 13-10-1993 | AT 153159 T | 15-05-1997 |
| | | AU 3533093 A | 07-10-1993 |
| | | CA 2087886 A,C | 07-10-1993 |
| | | DE 69310604 D | 19-06-1997 |
| | | DE 69310604 T | 04-09-1997 |
| | | ES 2101227 T | 01-07-1997 |
| | | HK 1002716 A | 11-09-1998 |
| | | JP 6046162 A | 18-02-1994 |
| | | US 5406619 A | 11-04-1995 |
| EP 0621570 A | 26-10-1994 | FR 2704081 A | 21-10-1994 |
| | | DE 69407647 D | 12-02-1998 |
| | | DE 69407647 T | 09-07-1998 |
| | | JP 7110876 A | 25-04-1995 |
| | | US 5495098 A | 27-02-1996 |
| DE 4138861 A | 01-10-1992 | NONE | |

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/F.. 01/00808

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/12 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie * | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| A | WO 97 22093 A (LANDIS & GYR)<br>19 juin 1997 (1997-06-19)<br>abrégé; revendications; figure 1<br>page 2, ligne 25 -page 3, ligne 28 | 1,3,4,6,<br>13-15 |
| A | EP 0 565 279 A (AMERICAN TELEPHONE AND TELEGRAPH) 13 octobre 1993 (1993-10-13)<br>abrégé; revendications; figure 5<br>page 5, ligne 9 - ligne 33 | 1,2,4,6 |
| A | EP 0 621 570 A (FRANCE TELECOM)<br>26 octobre 1994 (1994-10-26)<br>le document en entier | 1,4,6,7,<br>10-12 |
| A | DE 41 38 861 A (SIEMENS NIXDORF INFORMATIONSSYSTEME)<br>1 octobre 1992 (1992-10-01)<br>le document en entier | 1,4,6,<br>18,19 |

[ ] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 25 juin 2001 | 04/07/2001 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

1

## RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/00808

| Document brevet cité au rapport de recherche | | Date de publication | Membre(s) de la famille de brevet(s) | | Date de publication |
|---|---|---|---|---|---|
| WO 9722093 | A | 19-06-1997 | CH | 690530 A | 29-09-2000 |
| | | | AU | 704773 B | 06-05-1999 |
| | | | AU | 1140497 A | 03-07-1997 |
| | | | EP | 0870286 A | 14-10-1998 |
| EP 0565279 | A | 13-10-1993 | AT | 153159 T | 15-05-1997 |
| | | | AU | 3533093 A | 07-10-1993 |
| | | | CA | 2087886 A,C | 07-10-1993 |
| | | | DE | 69310604 D | 19-06-1997 |
| | | | DE | 69310604 T | 04-09-1997 |
| | | | ES | 2101227 T | 01-07-1997 |
| | | | HK | 1002716 A | 11-09-1998 |
| | | | JP | 6046162 A | 18-02-1994 |
| | | | US | 5406619 A | 11-04-1995 |
| EP 0621570 | A | 26-10-1994 | FR | 2704081 A | 21-10-1994 |
| | | | DE | 69407647 D | 12-02-1998 |
| | | | DE | 69407647 T | 09-07-1998 |
| | | | JP | 7110876 A | 25-04-1995 |
| | | | US | 5495098 A | 27-02-1996 |
| DE 4138861 | A | 01-10-1992 | AUCUN | | |